IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

EXPERT BUSINESS SYSTEMS, LLC, et al.,	:	
Plaintiffs	:	
	:	
v.	:	CIVIL NO. AMD 04-600
	:	
BI4CE, Inc., et al.,	:	
Defendants	:	

...o0o...

MEMORANDUM OPINION

Plaintiffs Expert Business Systems, LLC, and its principal, David Esaw, filed this case against defendants BI4CE, Inc., and its president, Christopher S. Chodnicki, seeking, in a seven-count complaint, substantial damages. Complete diversity of citizenship between the parties is absent; subject matter jurisdiction is based on federal question under 28 U.S.C. § 1331 and supplemental jurisdiction under 28 U.S.C. § 1367(c). One of plaintiffs' two federal claims arises under the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2521, namely, 18 U.S.C. § 2520(a)[1] and 18 U.S.C. § 2511[2] (the "interception

[1]Section 2520(a) creates a civil cause of action for violations of the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2521, and provides

> Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a). *See generally DIRECTV, Inc. v. Nicholas,* 403 F.3d 223, 225-26 (4th Cir.2005); *DIRECTV, Inc. v. Pepe*, 431 F.3d 162 (3d Cir. 2005). In this case, plaintiffs assert that defendants violated 18 U.S.C. § 2511 when they intercepted certain e-mails addressed to plaintiffs, disclosed the content of those e-mails, and used the information.

[2]Section 2511(a)(1) provides as follows in part:

> Except as otherwise specifically provided in this chapter any person who--

(continued...)

claim"). The second federal claim arises under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *See* 18 U.S.C. § 1030(g)[3] and 18 U.S.C. § 1030(a)(5)[4] (the "Trojan Horse

---

[2](...continued)

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> * * *
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
>
> * * *
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(a)(1).

[3]Section 1030(g) provides as follows in part:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.

18 U.S.C. § 1030(g).

[4]Section 1030(a)(5) provides as follows in pertinent part:

> (a) Whoever–
>
> * * *
>
> (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; * * * and
>
> (B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
>
> (i) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value;

(continued...)

claim").[5] The five state law claims are based on Maryland law. Defendants have filed state law counterclaims against plaintiffs.

Discovery having concluded, the parties have filed cross-motions for summary judgment. The issues have been briefed and a hearing is not necessary. For the reasons stated within, because defendants are entitled to judgment as a matter of law as to plaintiffs' federal claims, I shall direct the entry judgment thereon. Furthermore, the federal claims having been disposed of, I shall decline to exercise supplemental jurisdiction over the state law claims and those claims shall be dismissed without prejudice for lack of jurisdiction.

---

[4](...continued)

* * *

shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(5)(A)(i) & (B)(i).

[5]One website defines a Trojan Horse as follows:

> In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

SearchSecurity.com http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html (visited January 30, 2006). *See also* Symantec Security Response Website http://securityresponse.symantec.com/avcenter/refa.html#t (visited January 30, 2006):

> A Trojan Horse portrays itself as something other than what it is at the point of execution. While it may advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan Horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. A Trojan Horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort. The malicious functionality of a Trojan Horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

I.

The underlying dispute may be simply described. The parties are active in the information technology industry. By late 2002, plaintiffs had developed an early version of a software testing application called Test Plan Pro™ ("TPP") and wished to develop a more sophisticated TPP program, including a network-based version. After negotiations over several weeks, during which defendants evaluated the extant TPP application, the parties entered into a so-called "Teaming Agreement" on or about January 2, 2003, whereby, in return for a share of the profits from the marketing of the enhanced TPP application, defendants Chodnicki and his company, Bi4ce, Inc., another firm in the information technology industry, would work with plaintiffs in further developing TPP. The Teaming Agreement was in effect until plaintiffs terminated it in June 2003.[6]

During the pendency of the Teaming Agreement, defendants had unsupervised physical access to a desktop computer and a laptop computer owned by plaintiffs on at least one, and perhaps as many as three, occasions. According to plaintiffs, defendants were authorized solely to install a copy of the beta version of the enhanced TPP application on plaintiffs' computers. Defendants assert that, with either the express permission, or, at the least, the implicit permission of plaintiffs, they installed a remote access application to one

[6]The record shows that the relationship between the parties was, to put it delicately, unfulfilling. The record contains e-mails and other evidence indicating that plaintiff Esaw regularly used very harsh language toward defendants, including frequent sarcasm and threats. For their part, defendants (whose sole return under the Teaming Agreement was to be a share of profits on sales of the TPP, but who devoted well over 1,000 hours of development work on the product before it was ready for marketing) quickly developed a belief that plaintiffs were not devoting substantial efforts to the promotion of the TPP product, in contrast to their efforts at promoting the plaintiff corporation (a minority business enterprise) itself.

or both of the plaintiffs' computers, and they activated certain other features on one or both of them, such as instant messaging, so as to facilitate the parties' joint enterprise. For example, the remote access application permitted plaintiffs to access defendants' servers, which, by agreement of the parties during the Teaming Agreement, housed the TPP website and one or more other related websites critical to the further development and marketing of the TPP.

The overarching foundation of plaintiffs' theory of their federal claims is that as a result of the unauthorized installation of the remote access application on the plaintiffs' computers, defendants gave themselves secret, unauthorized access to the entirety of the business and personal computerized records and other data maintained by plaintiffs on their machines.[7] Of pertinence here, in any event, is plaintiffs' claim that, with or without secret access, defendants "intercepted" two e-mails intended for plaintiffs, and thereby violated 18 U.S.C. § 2511. Furthermore, according to plaintiffs, after plaintiffs advised defendants of their suspicions that defendants had accessed plaintiffs' computers without authority to do so through the use of the remote access program, defendants employed the remote access program to send a Trojan Horse to plaintiffs' desktop computer in order to destroy the evidence of defendants' unauthorized access, and thereby violated 18 U.S.C. § 1030(a)(5).

As elaborate as plaintiffs' theory of liability may be, their actual evidentiary support

---

[7]Indeed, much of plaintiffs' briefing and argument on the cross-motions for summary judgment can be read to suggest (as defendants seem to have assumed until plaintiffs filed their opposition memorandum) that *the mere unauthorized access* by defendants to plaintiffs' computers and/or *the mere installation of software on such computers without plaintiffs' express authorization* gives rise to a federal claim. This is not so, of course; only the two federal claims identified *supra*, nn. 1-4, having discrete statutory elements, have been asserted in this case.

for imposing liability on defendants under the federal claims consists merely of: (1) a rudimentary examination and ostensible analysis of the *images* of the hard drives of the two computers;[8] (2) an increasingly attenuated series of inferences-on-inferences based on circumstantial evidence arising from defendants' undisputed physical access to the plaintiffs' computers; (3) coupled with the undisputed evidence of frequent crashing and malfunctioning of plaintiffs' computers (resulting in loss of data) during the pendency of the Teaming Agreement and the months immediately after the Teaming Agreement had been terminated.[9]

Defendants vigorously deny that they gave themselves or exercised unauthorized access to plaintiffs' computers or that they intentionally (or unintentionally) damaged plaintiffs' computers, or that they ever attempted to do so. In particular, defendants assert (as to the interception claim) that they received the disputed e-mails in the ordinary course of business while the Teaming Agreement was in effect, just as they received countless transmissions of e-mails and other communications on plaintiffs' behalf attendant to the performance of their undertakings under the Teaming Agreement and maintenance and

---

[8]Plaintiffs assert that they were financially unable to retain an expert who could conduct the full forensic examination and report that would be needed to support their Trojan Horse claim.

[9]Plaintiffs employed two college-student interns during the relevant period. The interns had access to plaintiffs' computers and used and worked on them extensively, including software installations and updates, and other even more sophisticated changes. The expert opinion evidence in the record offered by defendants demonstrates as a matter of law that plaintiffs have not accurately set forth the date on which plaintiffs' interns first exercised dominion and control over plaintiffs' computers. Notably, one of the interns (apparently with plaintiffs' acquiescence) resisted defendants' efforts to depose him in this case and was never deposed.

operation of the TPP-related websites. Moreover, as to the Trojan Horse claim, defendants point to the absence of any expert opinion evidence based on the parties' respective forensic examinations of plaintiffs' computers to demonstrate either unauthorized access in general or any access by defendants leading to destruction of plaintiffs' software or hardware, in any event.

II.

Pursuant to Rule 56(c) of the Federal Rules of Civil Procedure, summary judgment is appropriate "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247 (1986). A fact is material for purposes of summary judgment, if, when applied to the substantive law, it affects the outcome of the litigation. *Id*. at 248. Summary judgment is also appropriate when a party "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Karim v. Staples, Inc.*, 210 F. Supp. 2d 737, 740 (D.Md. 2002).

III.

I am constrained to agree with defendants that the utter lack of any substantial probative evidence that defendants wrongfully "intercepted" the disputed e-mails fatally undercuts plaintiffs' interception claim. Moreover, the utter lack of any expert opinion evidence supporting the speculative assertions by plaintiffs that defendants sought and

obtained unauthorized access to plaintiffs' computers and thereby damaged the computers through the delivery of a Trojan Horse requires the court to enter summary judgment in favor of defendants on the Trojan Horse claims.

To survive summary judgment as to the interception claim, plaintiff must generate a dispute of material fact, *inter alia*, as to whether, given the undisputed background facts regarding the performance of the Teaming Agreement, including defendants hosting and maintenance of various websites and other data storage on their servers, either of the disputed two e-mails were intended to be delivered to plaintiffs without any involvement on the part of defendants. *Cf. United States v. Councilman*, 418 F.3d 67, 72-80 (1st Cir. 2005) (en banc) (explaining meaning of statutory terms "electronic communication" and "interception" as used in 18 U.S.C. § 2511 in criminal prosecution for intercepting e-mails). Even viewing the record in favor of plaintiffs as the non-movants, no reasonable juror could reasonably conclude by a preponderance of the evidence that defendants violated § 2511 when they received *and forwarded to plaintiffs* the disputed e-mails.[10]

As to the Trojan Horse claim, plaintiffs have not even attempted to respond to the unobjected-to and unrebutted opinion stated by defendants' forensic computer experts after they examined the allegedly corrupted computers: "[I]t is not possible to show any connection between [defendants'] activities and the alleged loss of data on the [desktop] .

[10]The disputed e-mails were addressed to fictional employees of plaintiffs, whose identities had been created by plaintiff Esaw to further his marketing efforts. As a matter of law, no reasonable juror could reasonably find by a preponderance of the evidence that defendants would have had an unlawful design in making inquiry about and then forwarding these e-mails to plaintiffs in the ordinary course of business during defendants' performance of tasks under the Teaming Agreement.

. . . [T]here is no evidence to support the claims [by plaintiffs] that [defendants] are responsible for any alleged data loss on [the desktop] machine." To put it plainly, there is no basis in the record for a reasonable juror to reach a contrary conclusion by a preponderance of the evidence.

IV.

For the reasons stated above, the defendants' motion for summary judgment shall be granted as to the federal claims. As complete diversity of citizenship is lacking in this case, I shall decline to exercise supplemental jurisdiction and shall dismiss without prejudice the remaining, state law claims. 28 U.S.C. § 1367(c)(3); *see generally Andrews v. Anne Arundel County, Md.,* 931 F.Supp. 1255, 1267-68 (D.Md.1996), *aff'd,* 114 F.3d 1175, 1997 WL 321573 (4th Cir.1997) (table), *cert. denied,* 522 U.S. 1015 (1997). An order follows.

Filed: January 31, 2006

/s/
ANDRE M. DAVIS
UNITED STATES DISTRICT JUDGE